ENTERPRISE FRAUD PORTAL

FRACTALS

FRACTALS

Every day, banks, payment processors and merchants protect their customers, their reputation and their bottom line from fraud using NCR's Fraud solution–Fractals.
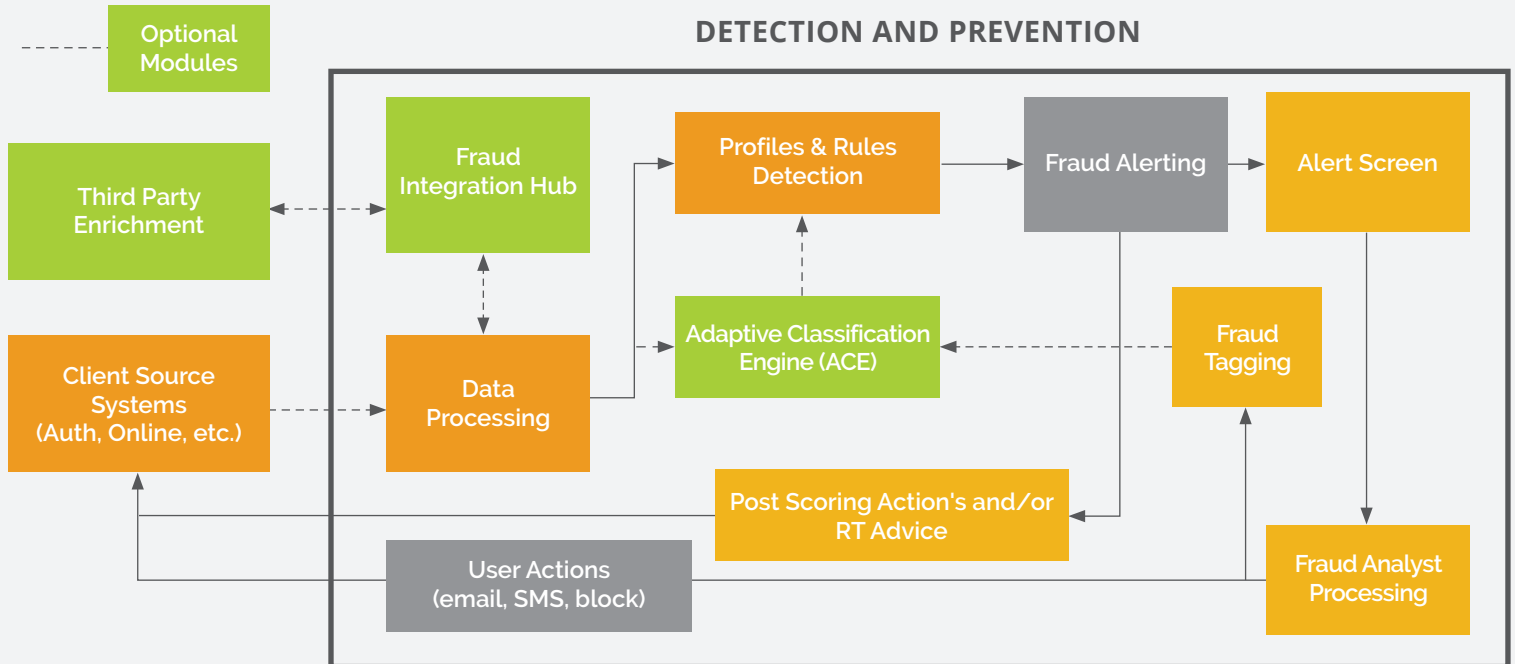
Fighting fraud is a continuous undertaking for companies and fraud management needs endless attention. Combine this task with the influx of growing electronic payment types and channels that your customers use and your company faces a perfect storm for the potential of damaging fraud attacks and increasing operational costs for fraud management.

Innovation in payment types and channels is challenged by fraudster innovation that is continuously updated with methods to maximize their profits. Fraud has become an international business and criminal gangs seek out the weakest targets for the easiest and highest returns.

For more information, visit us at ncr.com/Financial Services/Fraud.

FRACTALS SOLUTION CORE

DETECTION AND PREVENTION

Optional Modules

Third Party Enrichment

Client Source Systems (Auth, Online, etc.)

Fraud Integration Hub

Data Processing

Profiles & Rules Detection

Adaptive Classification Engine (ACE)

Fraud Alerting

Alert Screen

Fraud Tagging

Post Scoring Action's and/or RT Advice

User Actions (email, SMS, block)

Fraud Analyst Processing

Flexible, Efficient and Reduce Total Cost of Ownership

Taking a unified approach to fraud prevention and management, the Fractals portal supports the detection, analytics and management of fraud across users, accounts, products, and channels. Fractals combines analytical models with user-defined rules to give you an exceptionally high fraud detection rate with a low false positive ratio, helping your company reduce your total cost of fraud management. Fractals is flexible, scalable and easily configurable and is appropriate for companies of any size.

The NCR fraud solution gives you enterprise fraud detection and end-to end fraud competencies across all channels, all accounts and all payment types from a single portal. Your company can monitor transactions and assess historical and aggregated behavior across multiple accounts, multiple channels or groups of accounts.

Fractals enables you to enrich your fraud screening capabilities by incorporating data from the widest possible range of sources. In addition to the usual transactional information, you can include data from other internal systems and fraud-scoring models. Fractals also lets you take advantage of information provided by third parties, so you can validate the device, IP address and geo-location of the payment source.

When deployed with Authentic, NCR's payment processing platform, or any other payment engine, Fractals allows you to react to potential fraud in real-time, near real-time and batch mode.

NCR FRAUD SOLUTION MODULES

Fraud Integration Hub (FIH)

The Fraud Integration Hub takes payment transactions and event messages, in real time , and sends the relevant elements to your core systems and/or third party data sources to enrich the transaction data or log-on data. This is done prior to running any models or rules, allowing the user to have access to a much deeper set of data for the rules and strategies.

Classification Engine (ACE)

Fractals high fraud detection rate materializes because of Bayesian mathematical models detecting the probability of fraud, executing decisions in real-time as particular patterns arise in their transactional data.

The Adaptive Classification Engine can detect even the most subtle changes in fraud trends, enabling it to identify new fraud types as soon as they are activated and prevent them spreading further. ACE is flexible and is an open framework, giving users control over the fraud detection models, more so than other available solutions. ACE can analyze high-volume, multi-channel transactions and behavior activity with ease and contains strategies that self-adjust as transactions and behavior activity is tagged as fraudulent, which enables the model to learn new fraud patterns as they appear.

By constantly updating themselves, these self-adjusting models enable Fractals to keep up with even the most innovative of fraudsters, while minimizing input the required from your fraud analysts.

Dynamic Rules Engine

The Fractals rules engine enables you to define the rules which are used to score transactions and determine if a transaction should be authorized, declined or reviewed.

The rules engine is a browser-based interface where users define, create, test, evaluate and deploy rules. The graphical rule workbench is designed to make rule writing very straightforward for any level of user, making it easy to express complex and varied rules and providing the ability to update rules rapidly in response to changing threats

Post-scoring actions allow you to define automatic responses according to the outcome of the Adaptive Classification Engine or rules engine. If 'in flight' fraud prevention is needed, Fractals can return the appropriate response to the requesting system. Alternatively, Fractals can deliver a message to your communication partner or system of choice–via web service integration–on any account status change and/or non-financial event changes.

Alert Management

Once the Adaptive Classification Engine or the rules engine has identified a suspicious transaction, Fractals gives your fraud analysts the following support:

Alert queue management – a flexible, configurable mechanism for queuing alerts. Alerts can be grouped by common fraud score features, such as product type or transaction amount. Each analyst's queue can be linked to one or more alert groups, which provides a high degree of configurability to meet operational needs.

Alert handling – a browser-based interface for processing alerts. It provides fraud analysts with the data and analytical tools to fully understand customer behavior patterns.

Channel specific alert views displays the relevant data your analysts need to for a quick response. Giving the necessary information for each channel at the analysts fingertips allows your organization to improve analyst time efficiency.

Reporting

Fractals contains a comprehensive data warehouse that is built on the data housed within it.

Fractals has an ETL (extract transform load) script which will take the relevant data and send it to the reporting DB for aggregation and processing. This process allows your financial institution to create Ad-Hoc Reports on multiple aspects of a customer's data.

FRACTALS AT A GLANCE:

- Industry-leading fraud detection for banks, issuers, acquirers, PSPs, merchants and ISOs

- Real-Time, Near Real Time and Batch detection and prevention

- Easily configurable rules to create tailored risk management strategies

- Multi-channel, multi-tenant and multi-organization protection

- Complete channel and transaction coverage

- Ability to easily integrate data and disparate systems

FRACTALS BENEFITS:

- Gain ROI quicker as a result of simplified implementation

- Lower your Fraud Program Total Cost of Ownership– Efficient deployment and Integrations due to web-service capable solution suite

- Minimize false positives to maintain strong customer relationships

- Create tailored, granular and targeted risk management strategies and scores

- Generate cost savings and economies of scale from a single, scalable, automated solution

- Use your fraud analysts' time effectively to handle alert management, customer service, strategy development, trend analysis or business intelligence

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

NCR